

Vom Cyber Resilience Act zur CE-Kennzeichnung

Was Hersteller jetzt wissen müssen

5

Standorte

Berlin · Frankfurt
München · Leipzig · Wien

30

Security Experten

Berater · Forscher
Gutachter · Fachexperten

Kernkompetenzen

- Sicherheitskonzepte und -strategien
- Bedrohungs- und Risikoanalyse
- System Engineering
- Verifizierung, Validierung und Gutachten
- Pentesting und automatisierte Testausführung
- Test PKI-Infrastruktur und Zentrale Dienste
- Management, Schulung und Audits

Fachwissen zu Vorschriften und Normen

- IEC 62443 / ISO 27001
- CLC/TS 50701 / IEC 63452
- CENELEC EN 50126/50128/50129
- NIS 2 · CRA · CSA · BSI IT-SiG 2.0 · BSI-KritisV
- ERA System Pillar Cybersecurity

Gründer

Max Schubert

Geschäftsführer, Dipl.-Ing. (FH)



Prof. Dr. Stefan Katzenbeisser

Leiter Eisenbahnsicherheitsforschung, Gutachter



Prof. Dr. Christoph Krauß

Leiter Automobil-Sicherheitsforschung



NEXTRAIL GmbH

Experten für dem Bereich Eisenbahn





Martin Krabbe

Team Manager Cyber Security

Incyde Industrial Cyber Defense GmbH

Schwerpunkte

IEC 62443

SIEM/SOC/IDS

Cyber Resilience Act & NIS 2



VDMA

Aktive Mitarbeit im Verband



Incyde Industrial Cyber Defense GmbH

Team Manager – Industrielle Cybersicherheit und regulatorische Umsetzung



Informatik Consulting Systems GmbH

Head of Business Center Security



Bundeswehr

Cyber Security Engineer

01

Der CRA im Überblick

Ziele, Geltungsbereich, Rollen und Fristen

Verordnung (EU) 2024/2847

In Kraft seit 10.12.2024. Gilt unmittelbar in allen Mitgliedstaaten – ohne nationales Umsetzungsgesetz.

Horizontaler Ansatz

Erstmals verbindliche Cybersecurity-Anforderungen für nahezu alle Produkte mit digitalen Elementen – über den gesamten Lebenszyklus.

Teil der CE-Kennzeichnung

Cybersecurity wird zur Konformitätsanforderung – gleichrangig mit elektrischer Sicherheit oder EMV.

Security by Design wird zur Voraussetzung für den Marktzugang in der EU.



„Wer könnte heute Nacht eine aktiv ausgenutzte Schwachstelle innerhalb von 24 Stunden melden?“

11.09.2026

Meldepflicht aktiv

Aktiv ausgenutzte Schwachstellen und schwerwiegende Vorfälle müssen gemeldet werden – auch für Bestandsprodukte.

11.12.2027

CE nur noch mit CRA

Ohne Konformität mit dem Cyber Resilience Act keine CE-Kennzeichnung für Produkte mit digitalen Elementen.

Im Anwendungsbereich

- Hardware und Software mit direkter oder indirekter Datenverbindung zu einem Gerät oder Netz
- Inklusive zugehöriger Remote-Datenverarbeitung, z. B. das Cloud-Backend einer App
- Auch separat in Verkehr gebrachte Komponenten – Hardware und Software

Ausgenommen (Auszug)

- Medizinprodukte
- Kraftfahrzeuge, Luftfahrt, Schiffsausrüstung
- Produkte ausschließlich für nationale Sicherheit und Verteidigung
- Reiner SaaS-Betrieb ohne Produktbezug (→ NIS2)

Beispiele

Feldgeräte mit Ethernet

Edge-Gateways

Engineering-Software

Leitsystem-Komponenten

Hersteller

Hauptverantwortung

- Anforderungen aus Anhang I erfüllen
- Technische Dokumentation
- Konformitätsbewertung und CE
- Gesamter Supportzeitraum
- Meldungen an ENISA und CSIRT

Integrator

Kann selbst zum Hersteller werden

- Wer Komponenten zu einem neuen Produkt zusammenfügt und in Verkehr bringt, gilt als Hersteller
- Wesentliche Änderung durch Dritte: Herstellerpflichten für geänderten Teil
- Sorgfalt bei Fremd- und Open-Source-Komponenten
- SBOM, Updates und Supportzusagen vertraglich absichern

Betreiber

Keine direkten CRA-Pflichten

- Interne Nutzung lösen keine Herstellerpflichten aus
- Beschaffung: ab 11.12.2027 nur noch konforme Produkte innerhalb der EU
- Supportzeitraum: SBOM und Schwachstellenmanagement vertraglich regeln
- NIS2: CRA-Konformität als Nachweis der Lieferkettensicherheit

Wesentliche Änderung oder Vertrieb unter eigenem Namen macht auch Integratoren und Betreiber zum Hersteller, sobald sie das Produkt weitergeben. Maßgeblich ist die Änderung des Risikoprofils.

Aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle



Meldeweg

Single Reporting Platform: eine Meldung, Weiterleitung an die zuständigen CSIRTs und enisa

Bestandsprodukte

Gilt auch für Produkte, die schon vor 2027 auf dem Markt sind (Art. 69 Abs. 3)

Nutzer informieren

Betroffene Nutzer über Schwachstelle oder Vorfall und Abhilfemaßnahmen unterrichten

02

Produktklassifizierung

Die Klasse entscheidet über den Aufwand

Kritisch

Anhang IV

Wichtig

Anhang III · Klasse I und II

Standard

ca. 90 % aller Produkte

■ Kernfunktionalität entscheidet

Die Einordnung richtet sich nach der Hauptfunktion des Produkts – nicht nach jeder eingebauten Sicherheitsfunktion.

■ Strengeres Verfahren nach oben

Je höher die Kategorie, desto eher ist eine benannte Stelle oder Zertifizierung erforderlich.

■ Präzisierung durch die Kommission

Technische Beschreibungen der Kategorien werden per Durchführungsrechtsakt festgelegt.

Wichtig · Klasse I

- Betriebssysteme
- Router, Modems, Switches
- VPN-Produkte
- Netzwerkmanagementsysteme
- SIEM-Systeme
- Identitäts- und Zugriffsmanagement
- Mikrocontroller mit Sicherheitsfunktionen

Wichtig · Klasse II

- Firewalls
- Angriffserkennungs- und -abwehrsysteme (IDS/IPS)
- Hypervisoren und Container-Laufzeitsysteme
- Manipulationssichere Mikroprozessoren und Mikrocontroller

Kritisch · Anhang IV

- Hardware-Geräte mit Sicherheitsboxen
- Smart-Meter-Gateways
- Smartcards und Secure Elements

Maßgeblich ist die Kernfunktionalität – nicht jede eingebaute Sicherheitsfunktion macht ein Produkt „wichtig“.

Kategorie	Wer bewertet	Konsequenz
Standard	Hersteller selbst	Selbstbewertung, keine externe Stelle beteiligt
Klasse I	Hersteller selbst – nur mit harmonisierten Normen	Ohne gelistete Norm ist eine benannte Stelle erforderlich
Klasse II	Benannte Stelle	Externe Prüfung immer erforderlich
Kritisch	Benannte Stelle, künftig ggf. EU-Zertifizierung	Bis zu den delegierten Rechtsakten wie Klasse II

Bei Klasse I entscheidet die Normenlage – bislang ist keine harmonisierte CRA-Norm im Amtsblatt gelistet.



„Keine Security-Funktion – also Standard“

Betriebssystem, Routing oder VPN als Kernfunktion können trotzdem Klasse I auslösen.



Software und Firmware nicht betrachtet

Auch Firmware, Apps und separat vertriebene Softwarekomponenten sind Produkte mit digitalen Elementen.



Remote-Datenverarbeitung ignoriert

Das Cloud-Backend gehört zum Produkt und muss in Risikobewertung und Tests einbezogen werden.

03

Anforderungen

Anhang I: Produkt und Schwachstellenbehandlung



Keine bekannten Schwachstellen

Keine bekannten ausnutzbaren Schwachstellen beim Inverkehrbringen



Secure by Default

Sichere Standardkonfiguration, Rücksetzen auf Werkszustand



Zugriffsschutz

Authentifizierung und Schutz vor unbefugtem Zugriff



Vertraulichkeit und Integrität

Verschlüsselung, Schutz vor Manipulation



Datenminimierung

Nur die für den Zweck notwendigen Daten verarbeiten



Verfügbarkeit

Schutz wesentlicher Funktionen, auch bei DoS-Angriffen



Minimale Angriffsfläche

Schnittstellen begrenzen, Auswirkungen von Vorfällen eindämmen



Logging und Updates

Security-Protokollierung, automatische Updates mit Opt-out

Grundlage für die Umsetzungen ist die Cybersecurity-Risikoanalyse

Pflichten über den gesamten Supportzeitraum

1 SBOM

Maschinenlesbar, mindestens die Top-Level-Abhängigkeiten

2 Unverzüglich beheben

Schwachstellen ohne Verzögerung durch Updates beseitigen

3 Regelmäßig testen

Wirksame und regelmäßige Sicherheitsprüfungen

4 Transparenz

Behobene Schwachstellen öffentlich bekannt machen

5 Coordinated Vulnerability Disclosure-Policy

Richtlinie zur koordinierten Offenlegung und Kontaktstelle

6 Sichere Updates

Sichere Verteilung, Sicherheitsupdates kostenlos

≥ 5 Jahre

Mindest-Supportzeitraum

für die
Schwachstellenbehandlung inkl.
Sicherheitsupdates

10 Jahre

Abrufbarkeit je Sicherheitsupdate

Jedes veröffentlichte Update bleibt
ab Ausgabe mind. 10 Jahre
verfügbar – oder bis Supportende,
falls später

15–20 Jahre

Praxis: Nutzungsdauer in Anlagen

Erfahrungswert – Maßstab für die
Festlegung des Supportzeitraums

IEC 62443-4-1

Secure Development Lifecycle



Anhang I Teil II

Prozesse zur
Schwachstellenbehandlung

IEC 62443-4-2

Technische Anforderungen an
Komponenten



Anhang I Teil I

Produktanforderungen

60–70 %

erfüllt, wenn 62443-4-1/4-2
bereits implementiert

*Dies ist ein persönlicher
Erfahrungswert aus Projekten*

Gaps zwischen CRA und IEC 62443

- SBOM-Prozess
- Remote-Datenverarbeitung
- Meldeprozess (24 h)
- CE-Dokumentation
- Definierter Supportzeitraum
- Nutzerinformationen

04

Der Weg zur CE-Kennzeichnung

Von der Risikobewertung bis zur Konformitätserklärung



Cybersecurity-Risikobewertung

- Pflichtbestandteil der technischen Dokumentation
- Berücksichtigt Zweckbestimmung und Nutzung
- Umsetzung der Anforderungen aus Anhang I
- Aktualisierung über Lebenszyklus

Technische Dokumentation (Anhang VII)

- ✓ Allgemeine Produktbeschreibung
- ✓ Design, Entwicklung und Schwachstellenbehandlung
- ✓ Cybersecurity-Risikobewertung
- ✓ Begründung des Supportzeitraums
- ✓ Angewandte Normen und Spezifikationen
- ✓ Prüf- und Testberichte
- ✓ EU-Konformitätserklärung
- ✓ SBOM

Aufbewahrung: mind. 10 Jahre oder über den Supportzeitraum, falls länger

Modul A

Interne Kontrolle

Der Hersteller bewertet selbst, erstellt Dokumentation und erklärt die Konformität.

Geeignet für

Standardprodukte; Klasse I mit vollständig angewandten Normen

Modul B + C

Baumusterprüfung und Fertigungskontrolle

Benannte Stelle prüft Baumuster und Dokumentation (B),

Hersteller sichert die Serienfertigung (C).

Änderungen am Baumuster sind meldepflichtig.

Geeignet für

Klasse I ohne Normen; Klasse II

Modul H

Umfassende Qualitätssicherung

Benannte Stelle bewertet und überwacht QM-System für Entwicklung, Fertigung und Schwachstellenbehandlung –

Nicht jedes Baumuster einzeln prüfen

Geeignet für

Hersteller mit vielen Produkten und Varianten

Zertifizierung

Europäisches Schema nach dem Cybersecurity Act

Ein Zertifikat ab Stufe „substanziell“ (z. B. EUCC) begründet die Konformitätsvermutung, soweit es Anhang I abdeckt.

Geeignet für

Kritische Produkte – künftig ggf. verpflichtend

Bislang ist keine benannte Stelle für den CRA in NANDO gelistet – bis 11.12.2026 sollen ausreichend Stellen verfügbar sein.

Horizontal

EN 40000 · CEN-CLC/JTC 13 WG 9

- 1-1 Begriffe
- 1-2 Grundsätze der Cyber-Resilienz
- 1-3 Schwachstellenbehandlung
- 1-4 Generische Sicherheitsanforderungen

Listung zunächst v. a. für Teil 1-3 erwartet

Vertikal

je Produktkategorie

- **ETSI EN 304 6xx**
Eine Norm je Kategorie
- **prEN 50770 (CLC/TC 65X)**
OT-Profil für Firewalls, IDS/IPS, VPN, Router und Switches – auf Basis IEC 62443

Zeitplan

verschoben auf 31.10.2026

A-/B-Normen Schwachstellenbehandlung

verschoben auf 31.12.2026

C-Normen (produktspezifisch)

Herbst 2027

EN 40000-1-4 generische Anforderungen

Maschinenverordnung (EU) 2023/1230

Ab 20.01.2027: Schutz gegen Korruption und Sicherheit von Steuerungen

CRA-Konformität kann als Nachweis dienen.

Funkanlagenrichtlinie · Del. VO (EU) 2022/30

Seit 01.08.2025 mit EN 18031 – Basis der EN 40000.

CRA

NIS2

Betreiberpflichten ↔ Produktpflichten

Hersteller werden zu Lieferanten

Betreiber müssen die Security nachweisen

EU AI Act

Hochrisiko-KI mit CRA-Konformität erfüllt die Cybersecurity-Anforderungen, soweit abgedeckt.

EU AI ACT Erwägungsgrund 77

05

Praxis und Roadmap

Bisherige Herausforderungen, Fahrplan und ein Beispiel



Lieferkette

Zulieferer liefern keine SBOM oder keine Schwachstelleninformationen



Open Source

Komponenten ohne Pflegezusage oder mit unklarer Herkunft



Organisation

Security-Prozesse in der Entwicklung – aber nicht im Produktsupport



PSIRT

Meldeprozess braucht ein Product Security Incident Response Team – wir stellen dies nur selten fest



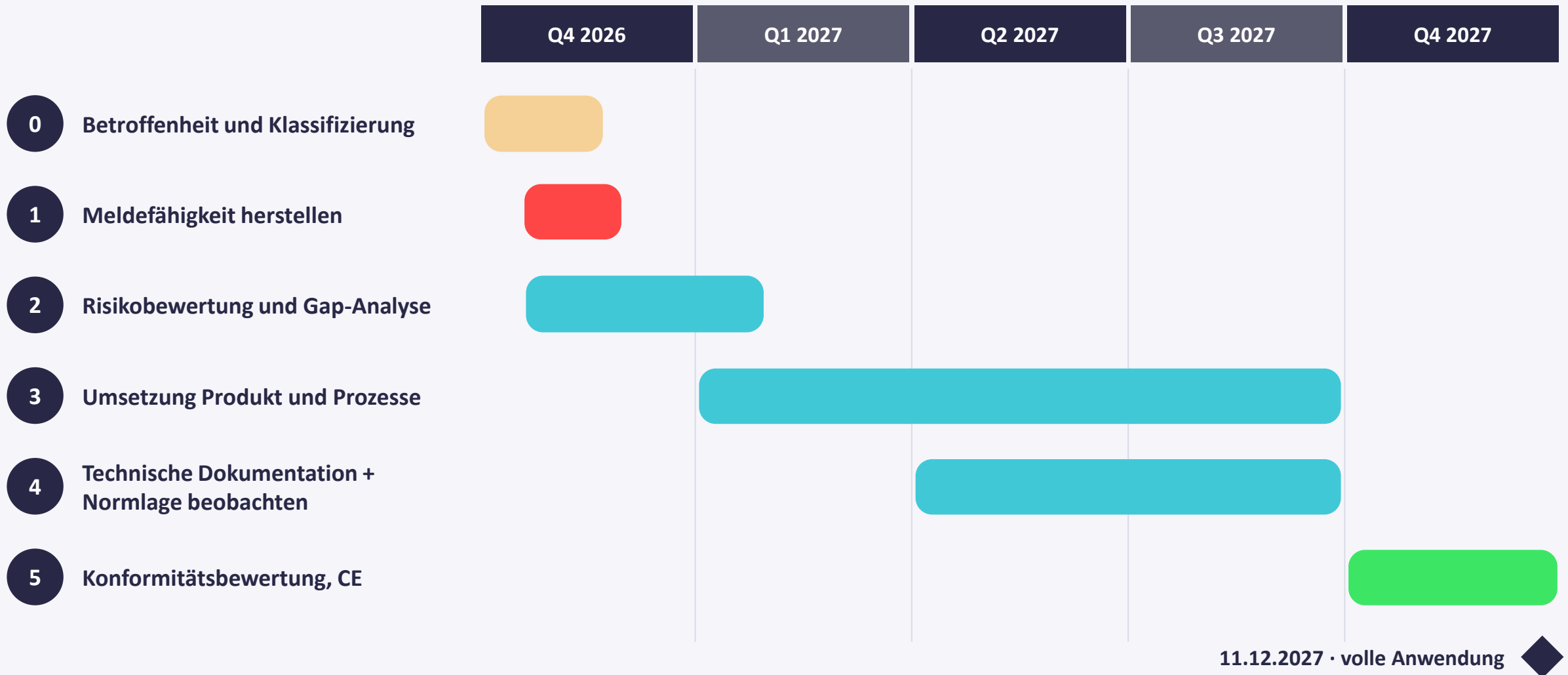
Kalkulation

Kosten für lange Supportzeiträume sind nicht eingepreist

12–24

Monate

realistische Projektlaufzeit bis zur Konformität



Phase	Kernaufgaben	Ergebnis
0 Klassifizierung	Produktinventar inkl. Software, Firmware und Cloud-Backends; Einordnung Standard / Klasse I / II / kritisch	Begründete Klassifizierung je Produkt
1 Meldefähigkeit	PSIRT benennen, 24/7-Eskalation, Registrierung auf der Single Reporting Platform	Meldung innerhalb 24 h möglich
2 Gap-Analyse	Risikobewertung, Abgleich gegen Anhang I Teil I und II	Priorisierte Maßnahmenliste
3 Umsetzung	Secure Defaults, signierte Updates, SBOM-Prozess, CVD-Policy, Supportzeitraum, Lieferantenverträge	Produkt und Prozesse CRA-fähig
4 Dokumentation	Technische Dokumentation nach Anhang VII, Normenstand prüfen, ggf. benannte Stelle beauftragen	Prüffähige Unterlagen
5 Bewertung	Modul A oder B+C / H, EU-Konformitätserklärung, CE-Kennzeichnung	Marktzugang ab 11.12.2027

01

Der CRA ist nicht erst 2027

Die Meldepflicht läuft bereits – auch für Bestandsprodukte.

02

Die Produktklasse entscheidet

Sie bestimmt Verfahren, Aufwand und ob eine benannte Stelle nötig ist.

03

IEC 62443 ist eine gute Basis

Aber nicht alles: SBOM, Meldeprozess und Supportzeitraum kommen hinzu.

04

Security wird Teil der CE

Und damit Teil von Marktzugang und Produktverantwortung.



Vielen Dank!

Fragen und Diskussion

Martin Krabbe · Incyde Industrial Cyber Defense GmbH · martin.krabbe@incyde.com